

AMENDMENTS TO THE CLAIMS

1 – 11 Cancelled

12. (original) A method of controlling a computer system, the computer system including a memory and at least one processor having at least three execution privilege levels, the execution privilege levels including a first privilege level, a second privilege level that is less privileged than the first privilege level, and a third privilege level that is less privileged than the second privilege level, the at least one processor also having protection key registers configured to hold protection keys that are employed to control access to security critical structures, the method comprising:

- operating a secure platform kernel (SPK) at the first privilege level as a privileged task;

- operating an operating system at the second privilege level as an unprivileged task;

- operating an end user application at the third privilege level as an unprivileged task;

- allocating a portion of the memory for use by the end user application;

- associating a first protection key value with the allocated memory portion;

- inserting the first protection key value in one of the protection key registers only when instructions of the end user application are being executed, thereby allowing the end user application to access the allocated memory portion and preventing other tasks operating at the second and the third privilege levels from accessing the allocated memory portion.

13. (original) The method of claim 12, and further comprising:

- monitoring execution of instructions of the end user application; and

- flushing the first protection key value from the protection key registers when execution of the end user application instructions stops.

14. (original) The method of claim 13, and further comprising:

reinserting the first protection key value in one of the protection key registers when execution of the end user application instructions resumes.

15. (original) The method of claim 12, wherein the allocating a portion of the memory is performed by the SPK.

16. (original) The method of claim 12, wherein the first protection key value is inserted in one of the protection key registers by the SPK.

17. (original) The method of claim 12, and further comprising:

associating a second protection key with the end user application to prevent unauthorized modification.

18 – 26 Cancelled.